

Claims

- [c1] 1.A method comprising:
- determining a set of accessor-accessible pairs, each accessor of each accessor-accessible pair having a predetermined level of access to the accessible of the accessor-accessible pair within a system topology; and,
- determining a mathematically canonical set of zones based on the set of accessor-accessible pairs, each zone having one or more accessors and one or more accessibles, the mathematically canonical set of zones used to manage access control of accessors and accessibles within the system topology.
- [c2] 2.The method of claim 1, wherein determining the mathematically canonical set of zones based on the set of accessor-accessible pairs comprises:
- for each unique accessible within the set of accessor-accessible pairs, sorting and merging accessors of the set of accessor-accessible pairs paired with the unique accessible as a first proto-zone, yielding a set of first proto-zones, each first proto-zone having one or more accessors and an accessible;
- for each unique one or more accessors within the set of first proto-zones, sorting and merging accessibles of the set of first proto-zones associated with the unique one or more accessors as a second proto-zone, yielding a set of second proto-zones, each second proto-zone having one or more accessors and one or more accessibles; and,
- sorting the set of second proto-zones to yield the mathematically canonical set of zones.
- [c3] 3.The method of claim 1, wherein determining the set of accessor-accessible pairs comprises determining each accessor-accessible pair, the accessor of each accessor-accessible pair having the predetermined level of access to the accessible of the accessor-accessible pair within the system topology according to each of one or more access control methods.
- [c4] 4.The method of claim 1, further comprising restoring access control of the accessors and accessibles within the system topology from a current configuration of the mathematically canonical set of zones to a target configuration of a second mathematically canonical set of zones.

[c5]

5.The method of claim 4, wherein restoring the access control from the current configuration to the target configuration comprises:

comparing the current configuration to the target configuration to yield a target-only canonical set of zones within only the target configuration, and a current-only canonical set of zones within only the current configuration;
removing zones common to both the target-only canonical set of zones and current-only canonical set of zones from both target-only and the current-only sets;

generating a create set of accessor-accessible pairs from the target-only canonical set of zones;

generating a remove set of accessor-accessible pairs from the current-only canonical set of zones;

removing any accessor-accessible pairs within both the create set and the remove set of accessor-accessible pairs from each of the create set and the remove set of accessor-accessible pairs;

for each accessor-accessible pair within the create set of accessor-accessible pairs, restoring the predetermined level of access of the accessor of the accessor-accessible pair to the accessible of the accessor-accessible pair within the system topology; and,

for each accessor-accessible pair within the remove set of accessor-accessible pairs, removing the predetermined level of access of the accessor of the accessor-accessible pair to the accessible of the accessor-accessible pair within the system topology.

[c6]

6.The method of claim 5, further comprising, after comparing the current configuration to the target configuration, ending the method upon determining that both the current-only set and the target-only canonical set of zones are empty.

[c7]

7.The method of claim 5, further comprising, after removing any accessor-accessible pairs within both the create set and the remove set of accessor-accessible pairs, ending the method upon determining that the at least one of the create set and the remove set of accessor-accessible pairs includes a pair having at least one of an accessor and an accessible absent in the system

topology.

[c8]

8.The method of claim 5, further comprising, after removing any accessor-accessible pairs within both the create set and the remove set of accessor-accessible pairs, ending the method upon determining that both the create set and the remove set of accessor-accessible pairs are empty.

[c9]

9.The method of claim 5, further comprising, after removing any accessor-accessible pair within both the create set and the remove set of accessor-accessible pairs, ending the method upon determining that at least one of any accessor-accessible pair within the create set of accessor-accessible pairs and any accessor-accessible pair within the remove set of accessor-accessible pairs cannot be realized within the system topology.

[c10]

10.The method of claim 4, wherein determining that any accessor-accessible pairs within the create set of accessor-accessible pairs cannot be realized within the system topology comprises at least one of:

determining that any accessor-accessible pairs within the create set of accessor-accessible pairs cannot be realized according to each of one or more access control methods within the system topology, where for the system topology, creation of access requires the access to be realizable by all the access control methods);

determining that any accessor-accessible pairs within the create set of accessor-accessible pairs cannot be realized according to all of the one or more access control methods within the system topology, where for the system topology, creation of access requires the access to be realizable by any of the access control methods;

determining that any accessor-accessible pairs within the create set of accessor-accessible pairs cannot be realized according to any constraints applicable to the system topology;

determining that any accessor-accessible pairs within the create set of accessor-accessible pairs cannot be realized according to each of the one or more access control methods within the system topology, where for the system topology, creation of access requires the access to be realizable by all access

control methods, without undesirably affecting the access level of any other accessor-accessible pair for the access control method; and,
determining that any accessor-accessible pairs cannot be realized according to all of the one or more access control methods within the system topology, where for the system topology, creation of access requires the access to be realizable by any of the access control methods, without undesirably affecting the access level of any other accessor-accessible pair for the access control method.

[c11]

11. The method of claim 4, wherein determining that any accessor-accessible pairs within the remove set of accessor-accessible pairs cannot be realized within the system topology comprises at least one of:

determining that any accessor-accessible pairs within the remove set of accessor-accessible pairs cannot be realized according to each of one or more access control methods within the system topology, where for the system topology, removal of access requires the access to be realizable by all the access control methods);

determining that any accessor-accessible pairs within the remove set of accessor-accessible pairs cannot be realized according to all of the one or more access control methods within the system topology, where for the system topology, removal of access requires the access to be realizable by any of the access control methods;

determining that any accessor-accessible pairs within the remove set of accessor-accessible pairs cannot be realized according to any constraints applicable to the system topology;

determining that any accessor-accessible pairs within the remove set of accessor-accessible pairs cannot be realized according to each of the one or more access control methods within the system topology, where for the system topology, removal of access requires the access to be realizable by all access control methods, without undesirably affecting the access level of any other accessor-accessible pair for the access control method; and,

determining that any accessor-accessible pairs cannot be realized according to all of the one or more access control methods within the system topology,

where for the system topology, removal of access requires the access to be realizable by any of the access control methods, without undesirably affecting the access level of any other accessor-accessible pair for the access control method.

[c12] 12.The method of claim 1, further comprising comparing a first configuration of the mathematically canonical set of zones to a second configuration of a second mathematically canonical set of zones.

[c13] 13.The method of claim 12, wherein comparing the first configuration to the second configuration comprises:
comparing the first configuration to the second configuration to yield at least a second-only canonical set of zones within only the second configuration, and a first-only canonical set of zones within only the first configuration;
removing the canonical set of zones common to both the second-only canonical set of zones and first-only canonical set of zones from both the first-only and the second-only sets;
upon determining that both the first-only set and the second-only canonical set of zones are empty, concluding that the first configuration is identical to the second configuration;
otherwise,

generating a second-only set of accessor-accessible pairs from the second-only canonical set of zones;
generating a first-only set of accessor-accessible pairs from the first-only canonical set of zones;
removing any accessor-accessible pairs within both the first-only set and the second-only set of accessor-accessible pairs from each of the first-only set and the second-only set of accessor-accessible pairs;
upon determining that both the first-only set and the second-only set of accessor-accessible pairs are empty, concluding that the first configuration is identical to the second configuration; and,
otherwise, concluding that the first configuration and the second configuration are different, as indicated by the first-only set and the second-only set of accessor-accessible pairs.

[c14]

14.A system comprising:

a plurality of accessibles within a topology accessible via at least one access control method;

a plurality of accessors within the topology, each accessor having a predetermined level of access to each of one or more of the plurality of accessibles via one or more of the at least one access control method; and, a computer-readable medium storing data representing a mathematically canonical representation of access of the plurality of accessors to the plurality of accessibles, the representation including at least one zone, each zone specifying one or more of the plurality of accessors having access to one or more of the plurality of accessibles,

the canonical representation satisfying a plurality of constraints comprising: a first constraint specifying that, for each zone, each of the one more accessors of the zone has identical access to each of the one or more accessibles of the zone;

a second constraint specifying that each of the plurality of accessibles belongs to no more than one of the at least one zone; and,

a third constraint specifying that the at least one zone encompass largest sets of the plurality of accessors that satisfy the first and the second constraints.

[c15]

15.The system of claim 14, further comprising a console by which the access of the plurality of accessors to the plurality of accessibles as represented by the mathematically canonical representation is manageable.

[c16]

16.The system of claim 15, wherein the console is one of the plurality of accessors.

[c17]

17.The system of claim 15, wherein the console permits a current configuration of the mathematically canonical representation to be restored to a target configuration of a second mathematically canonical representation.

[c18]

18.The system of claim 14, wherein the topology comprises one of: a storage-area network, and a communications network.

[c19]

19.An article of manufacture comprising:

a computer-readable medium; and,
means in the medium for managing access of a plurality of accessors within a system topology to a plurality of accessibles within the system topology by using a mathematically canonical set of zones, each zone specifying one or more of the plurality of accessors having access to one or more of the plurality of accessibles,
the canonical set of zones satisfying a plurality of constraints comprising:
a first constraint specifying that, for each zone, each of the one more accessors of the zone has identical access to each of the one or more accessibles of the zone;
a second constraint specifying that each of the plurality of accessibles belongs to no more than one zone; and,
a third constraint specifying that the canonical set of zones encompasses largest sets of the plurality of accessors that satisfy the first and the second constraints.

[c20]

20.The article of claim 19, wherein the medium is one of a recordable data storage medium and a modulated carrier signal.